10. Change sysadmin login ID to remove reverse xterm app-default.

2.2.2.3 SECMAN Changes:

The following changes were made to SECMAN:

Functions Added:

1. Changed default UB workstation security level to SECRET vice UNCLASS. This will allow CONFIDENTIAL and SECRET segments to load without error.

2. Tighten security so that UB will function with all user umask values set to 2 or 7 (current GCCS 2.2 plans call for umask 2). Assumes that users other than sysadmin and secman have a primary group of "gccs".

3. Modify the UB Export Users/Roles simply to export Roles, not users. This allows the system administrator to define UB roles and export them to the Tdbm clients, so that users have the same menus/permissions (e.g. track view vs. edit) on any machine.

Problems Corrected:

1. MACHINE environment variable corrected for SecAdm.

2.3 Known Discrepancies

1. During the system installation, when logging in after the first reboot (following GCCS COE load and System Configuration), a Warning window is displayed, indicating "Application Not Found". This is an anomaly related to the installation and will never appear once UB is loaded. It should be ignored.

2. Satellite database data cannot be transmitted.

3. The Views=>Set View Filter=>Apply button option will crash the System Chart, if the View window is not active (see Views=>Activate window).

   WORKAROUND: Always ensure the View window is active before selecting the Views=>Set View Filter=>Apply button option.

4. When loading an ADRG map, the user does not yet have the option to copy the ADRG to disk manually (i.e., to choose a target directory and copy the raw data across). All locally-loaded ADRGs reside in /home2/mapdata, and all global ADRGs reside in /h/data/global/mapdata.

5. Some software modifications made for UB3.0.1.6G may not yet be reflected in the online documentation. The VDD for 3.0.1.6G is, however available online, with the exception of last minute modifications.

6. Due to an EM/UB incompatibility issue, the Close All menu function is inoperative. Processes *are*, however, successfully terminated upon logout.

7. Tracks changed to DOTS via the various plot control mechanisms will not dynamically update their position until the normal symbol is redisplayed. This is a UB 3.0.1-release series deficiency, not specific to GCCS.

8. Many standard Ubfunction key operations are not available in GCCS (e.g., F4=Center Width).

   WORKAROUND: These same operations are available from the menu bar.

2.4 Other Notes

1. IMPORTANT: This version of UB includes Role-Based track management restriction capabilities. Users belonging to the default role, GCCS_Default, (likely including all existing users) are able to edit/add/delete/xmit tracks, and are also able to modify Elint Configuration.

   If there is a need for UB users with restrictions on track database management or on Elint Configuration, the system administrator must create and export a new role with the appropriate permissions, as follows:

   a. Log in as secman.
   b. Double-click the Roles icon.
   c. Add a new role (see Export Roles in the Unified Build 3.0.1.6G System Administrators Guide). Under the permissions section, check the Track and ElintConfig selections appropriately (Tracks: V=View-only, no editing; ElintConfig: E=Edit, allow editing)
   d. Export that role to all Tdbm clients (see Export Roles in the Unified Build 3.0.1.6G System Administrators Guide).
   e. Double-click the Security icon.
   f. Add a new user. In the "Role" field, select the newly-added role from the pick-list.

   The user created in Step f will have access as defined in Step c.

   Finally, it is important to understand the relationship between roles and segments that add menu-bar options. (Note: This does not affect segments using the Icon Launch Window.) The GCCS_DEFAULT, SA_DEFAULT, and SSO_DEFAULT roles are always given full permission to all menu items, including those from segments loaded after initial system configuration. Additionally, when new Roles are created, they are by default given permission to use all menu items. However, if Roles (other than the DEFAULTs) already exist when a menu-modifying segment is loaded, these Roles will, by default, NOT have permission to use the new menu options associated with that segment. The Role(s) must be edited (then likely exported) after the new segment load and permission granted, if these Roles require access to the new menu items.

WARNING: Do NOT attempt to create different roles for the System Administrator or Security Account Groups. Use the sysadmin and secman users provided with the software to access the needed functions.